

A metrical lower bound on the star discrepancy of digital sequences

Gerhard Larcher* and Friedrich Pillichshammer

Abstract

In this paper we study uniform distribution properties of digital sequences over a finite field of prime order. In 1998 it was shown by Larcher that for almost all s -dimensional digital sequences the star discrepancy D_N^* satisfies an upper bound of the form $D_N^* = O((\log N)^s (\log \log N)^{2+\varepsilon})$ for any $\varepsilon > 0$. Generally speaking it is much more difficult to obtain good lower bounds for specific sequences than upper bounds. Here we show that Larcher's result is best possible up to some $\log \log N$ term. More detailed, we prove that for almost all s -dimensional digital sequences the star discrepancy satisfies $D_N^* \geq c(q, s)(\log N)^s \log \log N$ for infinitely many $N \in \mathbb{N}$, where $c(q, s) > 0$ only depends on q and s but not on N .

1 Introduction and statement of the main result

In this paper we study uniform distribution properties of infinite sequences in the multi-dimensional unit cube. Sequences with excellent distribution properties are required as underlying nodes in so-called quasi-Monte Carlo algorithms for multivariate integration, see for example, [3, 7, 11] for more information in this direction.

Let $\mathcal{S} = (\mathbf{y}_n)_{n \geq 0}$ be an infinite sequence in the s -dimensional unit cube $[0, 1]^s$. For $\mathbf{x} = (x_1, \dots, x_s) \in [0, 1]^s$ and $N \in \mathbb{N}$ (by \mathbb{N} we denote the set of positive integers) the *local discrepancy* $D(\mathbf{x}, N)$ of \mathcal{S} is the difference between the number of indices $n = 0, \dots, N-1$ for which \mathbf{y}_n belongs to the interval $[\mathbf{0}, \mathbf{x}) = \prod_{j=1}^s [0, x_j)$ and the expected number $Nx_1 \cdots x_s$ of points in $[\mathbf{0}, \mathbf{x})$ if we assume a perfect uniform distribution on $[0, 1]^s$, i.e.,

$$D(\mathbf{x}, N) = \#\{0 \leq n < N : \mathbf{y}_n \in [\mathbf{0}, \mathbf{x})\} - Nx_1 \cdots x_s.$$

A sequence \mathcal{S} is called *uniformly distributed* if and only if for any $\mathbf{x} \in [0, 1]^s$ the normalized local discrepancy $D(\mathbf{x}, N)/N$ tends to 0 for growing N . The *star discrepancy* D_N^* of a sequence \mathcal{S} is the L_∞ -norm of the local discrepancy, i.e.,

$$D_N^*(\mathcal{S}) = \|D(\mathbf{x}, N)\|_\infty.$$

It follows from a result of Roth [12] that there exists a quantity $c(s) > 0$ such that for any sequence \mathcal{S} in $[0, 1]^s$ we have

$$D_N^*(\mathcal{S}) \geq c(s)(\log N)^{s/2} \quad \text{for infinitely many } N \in \mathbb{N}. \quad (1)$$

*G. L. is partially supported by the Austrian Science Foundation (FWF), project P21943-N18

For a proof, see, for example, [7, Chapter 2, Theorem 2.2]. However, the exact lower order of star discrepancy in N is still one of the most famous open problems in the theory of uniform distribution. Many people believe that there exists some $c(s) > 0$ such that for any infinite sequence \mathcal{S} in $[0, 1]^s$ we have

$$D_N^*(\mathcal{S}) \geq c(s)(\log N)^s \quad \text{for infinitely many } N \in \mathbb{N}. \quad (2)$$

Until now it is not known whether this conjecture is true for any $s \geq 2$. For dimension $s = 1$ the correctness of (2) has been shown by Schmidt [13]. If the conjectured lower bound (2) is correct, then it would be best possible in the order of magnitude in N . An excellent introduction to this topic can be found in the book of Kuipers and Niederreiter [7]. Further books dealing with uniform distribution theory, discrepancy and applications are [2, 3, 4, 9, 11] which can also be warmly recommended.

One example of sequences which can achieve a discrepancy bound of order of magnitude $(\log N)^s$ in N are so-called digital sequences over a finite field \mathbb{F}_q of prime-power order q . Such sequences go back to Sobol' [14] and Faure [5], but the detailed introduction and investigation of the general concept was first given by Niederreiter in [10]. In the following we always assume that q is a prime number. Hence we can identify \mathbb{F}_q with $\mathbb{Z}_q = \{0, 1, \dots, q-1\}$ equipped with arithmetic operations modulo q . By $(\mathbb{Z}_q^{\mathbb{N}})^{\top}$ we will denote the set of infinite dimensional column vectors over \mathbb{Z}_q .

Definition 1 (digital sequences). Let $s \in \mathbb{N}$ and q be a prime number. Let $C_1, \dots, C_s \in \mathbb{Z}_q^{\mathbb{N} \times \mathbb{N}}$ be $\mathbb{N} \times \mathbb{N}$ matrices over \mathbb{Z}_q . Let $n \in \mathbb{N}_0$, where $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$, with q -adic expansion $n = n_0 + n_1q + n_2q^2 + \dots$ (this expansion is obviously finite) and set

$$\vec{n} = (n_0, n_1, n_2, \dots)^{\top} \in (\mathbb{Z}_q^{\mathbb{N}})^{\top}.$$

Then define

$$\vec{x}_{n,j} = C_j \vec{n} \quad \text{for } j = 1, \dots, s$$

where all arithmetic operations are taken modulo q . Let $\vec{x}_{n,j} = (x_{n,j,1}, x_{n,j,2}, \dots)^{\top}$ and define

$$x_{n,j} = x_{n,j,1}q^{-1} + x_{n,j,2}q^{-2} + \dots$$

Then the n th point \mathbf{x}_n of the sequence $\mathcal{S}(C_1, \dots, C_s)$ is given by $\mathbf{x}_n = (x_{n,1}, \dots, x_{n,s})$. A sequence $\mathcal{S}(C_1, \dots, C_s)$ constructed this way is called a *digital sequence (over \mathbb{Z}_q)* with generating matrices C_1, \dots, C_s .

Under certain conditions on the generating matrices it can be shown that the star discrepancy of $\mathcal{S}(C_1, \dots, C_s)$ is of order of magnitude $(\log N)^s$ in N . For more information we refer to [3, 10, 11] and the references therein. Lower bounds for the star discrepancy of digital sequences are difficult to prove and until now we only have the general lower bound (1) for arbitrary sequences, but no specific results or even improvements for digital sequences. There is only a single result in dimension $s = 2$ due to Faure [6] who showed for one specific $(0, 2)$ -sequence over \mathbb{Z}_2 the lower bound

$$\limsup_{N \rightarrow \infty} \frac{D_N^*(\mathcal{S})}{(\log N)^2} \geq \frac{1}{24(\log 2)^2}.$$

In this paper we are interested in metrical results for the star discrepancy of digital sequences. For metrical problems we need a suitable probability measure on the set of all s -tuples of $\mathbb{N} \times \mathbb{N}$ matrices over \mathbb{Z}_q . We introduce this probability measure in three steps:

- First, let $\tilde{\mu}$ be the measure on the sequence space $\mathbb{Z}_q^{\mathbb{N}}$ induced by the equiprobability measure on \mathbb{Z}_q .
- Then, to define a probability measure μ on $\mathbb{Z}_q^{\mathbb{N} \times \mathbb{N}}$, we consider the set $\mathbb{Z}_q^{\mathbb{N} \times \mathbb{N}}$ of all infinite matrices over \mathbb{Z}_q as the product of denumerable many copies of the sequence space $\mathbb{Z}_q^{\mathbb{N}}$ over \mathbb{Z}_q , and define μ as the product measure induced by $\tilde{\mu}$ on $\mathbb{Z}_q^{\mathbb{N}}$.
- Finally, the probability measure μ_s on set $(\mathbb{Z}_q^{\mathbb{N} \times \mathbb{N}})^s$ of all s -tuples of $\mathbb{N} \times \mathbb{N}$ matrices over \mathbb{Z}_q is the s -fold product measure induced by the probability measure μ on the set $\mathbb{Z}_q^{\mathbb{N} \times \mathbb{N}}$.

Remark 1. Let us remark the following concerning the measure $\tilde{\mu}$. We can identify each $\vec{c} = (c_1, c_2, \dots) \in \mathbb{Z}_q^{\mathbb{N}}$ with its generating function $L = \sum_{k=1}^{\infty} c_k z^{-k} \in \mathbb{Z}_q((z^{-1}))$, where $\mathbb{Z}_q((z^{-1}))$ is the field of formal Laurent series over \mathbb{Z}_q in the variable z^{-1} . In this way we can identify $\mathbb{Z}_q^{\mathbb{N}}$ with the set H of all generating functions. Consider the *discrete exponential valuation* $\tilde{\nu}$ on H which is defined by $\tilde{\nu}(L) = -w$ if $L \neq 0$ and w is the least index with $c_w \neq 0$. For $L = 0$ we set $\tilde{\nu}(0) = -\infty$. With the topology induced by the discrete exponential valuation $\tilde{\nu}$ and with respect to addition, H is a compact abelian group, and $\tilde{\mu}$ then is the unique Haar probability measure on H .

With the probability measure μ_s at hand Larcher [8] proved the following metrical upper bound on the star discrepancy of digital sequences:

Theorem 1 (Larcher, 1998). *Let $s \in \mathbb{N}$, let q be a prime number and let $\varepsilon > 0$. Then for μ_s -almost all s -tuples $(C_1, \dots, C_s) \in (\mathbb{Z}_q^{\mathbb{N} \times \mathbb{N}})^s$ of generating matrices the digital sequence $\mathcal{S}(C_1, \dots, C_s)$ over \mathbb{Z}_q has star discrepancy satisfying*

$$D_N^*(\mathcal{S}(C_1, \dots, C_s)) \leq c(q, s, \varepsilon)(\log N)^s (\log \log N)^{2+\varepsilon}$$

with some $c(q, s, \varepsilon) > 0$ not depending on N .

This means that μ_s -almost all digital sequences achieve the conjectured best possible bound on the star discrepancy up to some $\log \log N$ term.

In this paper we will show that the result of Theorem 1 is best possible (up to some $\log \log N$ term). We will prove:

Theorem 2. *Let $s \in \mathbb{N}$ and let q be a prime number. Then for μ_s -almost all s -tuples $(C_1, \dots, C_s) \in (\mathbb{Z}_q^{\mathbb{N} \times \mathbb{N}})^s$ of generating matrices the digital sequence $\mathcal{S}(C_1, \dots, C_s)$ over \mathbb{Z}_q has star discrepancy satisfying*

$$D_N^*(\mathcal{S}(C_1, \dots, C_s)) \geq c(q, s)(\log N)^s \log \log N \quad \text{for infinitely many } N \in \mathbb{N}$$

with some $c(q, s) > 0$ not depending on N .

For the proof of the result we use an approach similar to the technique used by Beck [1] to give a metric lower bound for the discrepancy of Kronecker sequences.

2 Auxiliary results

We begin with some basic notations. Throughout the paper let q be a prime number and let $s \in \mathbb{N}$. Let $C, C_1, C_2, \dots \in \mathbb{Z}_q^{\mathbb{N} \times \mathbb{N}}$ and let $k, \ell, k_1, k_2, \dots \in \mathbb{N}_0$. By $\vec{k}, \vec{\ell}, \vec{k}_1, \vec{k}_2, \dots$ we denote the digit vectors of k, ℓ, k_1, k_2, \dots in base q , respectively, i.e., for $k = \kappa_0 + \kappa_1 q + \dots + \kappa_r q^r$ with $\kappa_r \neq 0$ we set

$$\vec{k} = (k_0, k_1, \dots, k_r, 0, \dots)^\top \in (\mathbb{Z}_q^{\mathbb{N}})^\top$$

and we define

$$\text{len}_q(k) = \text{len}_q(\vec{k}) := r = \lfloor \log_q k \rfloor.$$

For $k_1, k_2 \in \mathbb{N}_0$ we write $k_1 \oplus k_2$ for the integer with digit vector $\vec{k}_1 + \vec{k}_2$, where the addition of digit vectors is always component wise modulo q . By C^\top we denote the transpose of the matrix C .

An important tool in our analysis are q -adic Walsh functions which we introduce now:

Definition 2 (q -adic Walsh functions). Let q be a prime number and let $\omega_q := \exp(2\pi i/q)$ be the q th root of unity. For $j \in \mathbb{N}_0$ with q -adic expansion $j = j_0 + j_1 q + j_2 q^2 + \dots$ (this expansion is obviously finite) the j th q -adic *Walsh function* ${}_q\text{wal}_j : \mathbb{R} \rightarrow \mathbb{C}$, periodic with period one, is defined as

$${}_q\text{wal}_j(x) = \omega_q^{j_0 \xi_1 + j_1 \xi_2 + j_2 \xi_3 + \dots}$$

whenever $x \in [0, 1)$ has q -adic expansion of the form $x = \xi_1 q^{-1} + \xi_2 q^{-2} + \xi_3 q^{-3} + \dots$ (unique in the sense that infinitely many of the digits ξ_i must be different from $q - 1$).

In the following it is sometimes convenient to use the following notation: to $x \in [0, 1)$ with q -adic expansion of the form $x = \xi_1 q^{-1} + \xi_2 q^{-2} + \xi_3 q^{-3} + \dots$ we associate its q adic digit vector

$$\vec{x} = (\xi_1, \xi_2, \xi_3, \dots)^\top$$

and then we write

$${}_q\text{wal}_j(\vec{x}) := {}_q\text{wal}_j(x).$$

For a vector $\vec{b} = (b_1, b_2, \dots)^\top \in (\mathbb{Z}_q^{\mathbb{N}})^\top$ we say $\nu(\vec{b}) = -w$ if it is of the form

$$\vec{b} = (0, 0, \dots, 0, b_w, b_{w+1}, \dots)^\top \quad \text{with } b_w \neq 0.$$

In the following lemma we collect some useful properties of Walsh functions which we require for the proof of Theorem 2. More information on Walsh functions can be found in [3, Appendix A].

Lemma 1. *We have*

$$1. \quad {}_q\text{wal}_j(C_1 \vec{k}_1 + C_2 \vec{k}_2) = {}_q\text{wal}_j(C_1 \vec{k}_1) {}_q\text{wal}_j(C_2 \vec{k}_2);$$

2.

$$\sum_{x=0}^{q^m-1} {}_q\text{wal}_k(x/q^m) \overline{{}_q\text{wal}_\ell(x/q^m)} = \begin{cases} 1 & \text{if } \nu(\vec{k} - \vec{\ell}) < -m, \\ 0 & \text{otherwise,} \end{cases}$$

(orthonormality of Walsh functions); and

3.

$$\int_{\mathbb{Z}_q^{\mathbb{N} \times \mathbb{N}}} {}_q\text{wal}_i(C^\top \vec{k}) d\mu(C) = \begin{cases} 1 & \text{if } i = 0 \text{ or } \vec{k} = \vec{0}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Point 1. and 2. are standard properties of Walsh functions and are easily deduced from their definition (see also [3, Appendix A]). The assertion of 3. is clear whenever $i = 0$ or $k = 0$. Assume now that $i \neq 0$ and $k \neq 0$ with q -adic digit expansions $i = i_0 + i_1q + \dots + i_{r-1}q^{r-1}$ and $k = k_0 + k_1q + \dots + k_{m-1}q^{m-1}$, respectively. Then we have

$$\int_{\mathbb{Z}_q^{\mathbb{N} \times \mathbb{N}}} {}_q\text{wal}_i(C^\top \vec{k}) d\mu(C) = \prod_{a=0}^{r-1} \prod_{b=0}^{m-1} \sum_{c=0}^{q-1} \omega_q^{c i_a k_b}.$$

Since i, k are both different from zero, there exist a, b such that $i_a k_b \neq 0$ and for this choice we have $\sum_{c=0}^{q-1} \omega_q^{c i_a k_b} = 0$ and the result follows. \square

Now we present a series of auxiliary lemmas for the proof of Theorem 2.

Lemma 2. For $m \in \mathbb{N}$ and $k_1, \dots, k_s \in \mathbb{N}_0$, not all of them 0, let

$$M_m(k_1, \dots, k_s) := \{(C_1, \dots, C_s) \in (\mathbb{Z}_q^{\mathbb{N} \times \mathbb{N}})^s : \nu(C_1^\top \vec{k}_1 + \dots + C_s^\top \vec{k}_s) \leq -m\}.$$

Then we have

$$\mu_s(M_m(k_1, \dots, k_s)) = \frac{1}{q^{m-1}}.$$

Proof. Let χ be the characteristic function of the interval $[0, q^{-(m-1)})$. Then, according to [3, Lemma 3.9], χ has a finite Walsh series representation in base q of the form

$$\chi(x) = \sum_{i=0}^{q^{m-1}-1} a_i {}_q\text{wal}_i(x)$$

with $a_0 = q^{-(m-1)}$. In the following we identify x with its q -adic digit vector \vec{x} and we write $\chi(\vec{x}) := \chi(x)$. With this notation we have

$$\begin{aligned} \mu(M_m(k_1, \dots, k_s)) &= \int_{(\mathbb{Z}_q^{\mathbb{N} \times \mathbb{N}})^s} \chi(C_1^\top \vec{k}_1 + \dots + C_s^\top \vec{k}_s) d\mu_s(C_1, \dots, C_s) \\ &= a_0 + \sum_{i=1}^{q^{m-1}-1} a_i \int_{(\mathbb{Z}_q^{\mathbb{N} \times \mathbb{N}})^s} {}_q\text{wal}_i(C_1^\top \vec{k}_1 + \dots + C_s^\top \vec{k}_s) d\mu_s(C_1, \dots, C_s) \\ &= \frac{1}{q^{m-1}} + \sum_{i=1}^{q^{m-1}-1} a_i \prod_{j=1}^s \int_{\mathbb{Z}_q^{\mathbb{N} \times \mathbb{N}}} {}_q\text{wal}_i(C_j^\top \vec{k}_j) d\mu(C_j) \\ &= \frac{1}{q^{m-1}}, \end{aligned}$$

according to Lemma 1, since at least one of the \vec{k}_j is different from $\vec{0}$. \square

For $\mathbf{k} = (k_1, \dots, k_s) \in \mathbb{N}_0^s$ and $\boldsymbol{\ell} = (\ell_1, \dots, \ell_s) \in \mathbb{N}_0^s$ we say that \mathbf{k} and $\boldsymbol{\ell}$ are strongly dependent over \mathbb{Z}_q if there is a $c \in \mathbb{Z}_q \setminus \{0\}$ such that

$$\vec{k}_i = c \vec{\ell}_i \quad \text{for all } i = 1, \dots, s.$$

Lemma 3. For $\mathbf{k} = (k_1, \dots, k_s) \in \mathbb{N}_0^s$ and $\boldsymbol{\ell} = (\ell_1, \dots, \ell_s) \in \mathbb{N}_0^s$ we have

$$\prod_{u=1}^s \int_{\mathbb{Z}_q^{\mathbb{N} \times \mathbb{N}}} {}_q\text{wal}_i(C_u^\top \vec{k}_u) {}_q\text{wal}_j(C_u^\top \vec{\ell}_u) d\mu(C_u) = 1$$

if and only if we are in one of the following cases:

1. $i = j = 0$; or
2. $k_u = \ell_u = 0$ for all $u = 1, \dots, s$; or
3. $j = 0$ and $k_u = 0$ for all $u = 1, \dots, s$; or
4. $i = 0$ and $\ell_u = 0$ for all $u = 1, \dots, s$; or
5. $\vec{j} = c\vec{i}$ and $\vec{k}_u = c\vec{\ell}_u$ for all $u = 1, \dots, s$ for some $c \in \mathbb{Z}_q \setminus \{0\}$.

In all other cases the above product equals 0.

Proof. The assertion is clear whenever $i = j = 0$, this is item 1. Let

$$\begin{aligned} \vec{k}_u &= (k_{u,0}, k_{u,1}, \dots)^\top \\ \vec{\ell}_u &= (\ell_{u,0}, \ell_{u,1}, \dots)^\top \\ \vec{i} &= (i_0, i_1, \dots)^\top \\ \vec{j} &= (j_0, j_1, \dots)^\top \end{aligned}$$

be the q -adic digit vectors of k_u, ℓ_u, i and j , respectively. By the definition of Walsh functions it easily follows that

$${}_q\text{wal}_i(C_u^\top \vec{k}_u) {}_q\text{wal}_j(C_u^\top \vec{\ell}_u) = \prod_{a,b=0}^{\infty} \omega_b^{c_{u,b+1,a+1}(k_{u,a}i_b + \ell_{u,a}j_b)},$$

where $c_{u,a,b}$ is the element in the a th row and b th column of the matrix C_u . Note that this product is in fact a finite product since the components of the vectors $\vec{k}_u, \vec{\ell}_u, \vec{i}, \vec{j}$ become eventually 0.

Hence the product from the lemma is 1 if and only if

$$k_{u,a}i_b + \ell_{u,a}j_b = 0 \quad \text{for all } u = 1, \dots, s \text{ and } a, b \in \mathbb{N}_0$$

and it is 0 in all other cases.

If i and j not both are zero, then we may assume without loss of generality that there is a b such that $i_b \neq 0$. Hence

$$k_{u,a} = (-i_b^{-1}j_b)\ell_{u,a} \quad \text{for all } a \in \mathbb{N}_0 \text{ and } u = 1, \dots, s.$$

With $c := -i_b^{-1}j_b$ we obtain $\vec{k}_u = c\vec{\ell}_u$ for all $u = 1, \dots, s$.

Further, if $i_b = 0$ for some b , then

$$\ell_{u,a}j_b = 0 \quad \text{for all } a \in \mathbb{N}_0 \text{ and } u = 1, \dots, s$$

and hence $j_b = 0$ or $\vec{l}_u = \vec{0}$ for all $u = 1, \dots, s$. To summarize: If not all $\vec{\ell}_u$ are equal to $\vec{0}$, then $i_b = 0$ implies $j_b = 0$ and therefore $i_b c = j_b$ holds for all $b \in \mathbb{N}_0$, i.e.,

$$\vec{j} = c\vec{i}.$$

This proves item 5.

If the $\vec{\ell}_u$ are all equal to $\vec{0}$, then the product reduces to

$$\prod_{u=1}^s \int_{\mathbb{Z}_q^{\mathbb{N} \times \mathbb{N}}} q^{\text{wal}_i(C_u^\top \vec{k}_u)} d\mu(C_u)$$

and this is equal to one, iff $i = 0$ (item 4.) or $\vec{k}_u = \vec{0}$ for all $u = 1, \dots, s$ (item 2.). Item 3. follows in the same way as item 4. \square

Lemma 4. *Let $\overline{P} \subseteq \mathbb{N}^s$. For $(k_1, \dots, k_s) \in \overline{P}$ with $\text{len}_q(k_j) = r_j$ for $j = 1, \dots, s$ let $\beta_1(k_1), \dots, \beta_s(k_s) \in \mathbb{N}_0$ with $\beta_j(k_j) = 0$ or $\text{len}_q(\beta_j(k_j)) > \text{len}_q(k_j)$ for all $j = 1, \dots, s$ but not all of them equal to zero. Let*

$$\begin{aligned} \widetilde{M} &:= \{(C_1, \dots, C_s) \in (\mathbb{Z}_q^{\mathbb{N} \times \mathbb{N}})^s : \nu(C_1^\top \vec{k}_1 + \dots + C_s^\top \vec{k}_s) \leq -(r_1 + \dots + r_s), \\ &\quad \nu(C_1^\top (\vec{k}_1 + \vec{\beta}_1(k_1)) + \dots + C_s^\top (\vec{k}_s + \vec{\beta}_s(k_s))) \leq -\lfloor (r_1 + \dots + r_s)/2 \rfloor \\ &\quad \text{for infinitely many } (k_1, \dots, k_s) \in \overline{P}\}. \end{aligned}$$

Then we have

$$\mu_s(\widetilde{M}) = 0.$$

Proof. For given $k_1, \dots, k_s \in \mathbb{N}$ not all $k_j = 1$ let

$$M_1(k_1, \dots, k_s) := \{(C_1, \dots, C_s) : \nu(C_1^\top \vec{k}_1 + \dots + C_s^\top \vec{k}_s) \leq -(r_1 + \dots + r_s)\}$$

and

$$\begin{aligned} M_2(k_1, \dots, k_s) &:= \left\{ (C_1, \dots, C_s) : \right. \\ &\quad \left. \nu(C_1^\top (\vec{k}_1 + \vec{\beta}_1(k_1)) + \dots + C_s^\top (\vec{k}_s + \vec{\beta}_s(k_s))) \leq -\left\lfloor \frac{r_1 + \dots + r_s}{2} \right\rfloor \right\}. \end{aligned}$$

We use the notation $m := r_1 + \dots + r_s$. Let χ_1 be the characteristic function of the interval $[0, q^{-(m-1)})$ and let χ_2 be the characteristic function of the interval $[0, q^{-(\lfloor m/2 \rfloor - 1)})$. Again by [3, Lemma 3.9] we have finite Walsh series representations for χ_1 and χ_2 in base q given by

$$\chi_1 = \sum_{i=0}^{q^{m-1}-1} a_i^{(1)} q^{\text{wal}_i} \quad \text{and} \quad \chi_2 = \sum_{i=0}^{q^{\lfloor m/2 \rfloor - 1} - 1} a_i^{(2)} q^{\text{wal}_i}$$

with

$$a_0^{(1)} = \frac{1}{q^{m-1}} \quad \text{and} \quad a_0^{(2)} = \frac{1}{q^{\lfloor m/2 \rfloor - 1}}.$$

Now we have

$$\mu_s(M_1(k_1, \dots, k_s) \cap M_2(k_1, \dots, k_s))$$

$$\begin{aligned}
&= \int_{(\mathbb{Z}_q^{\mathbb{N} \times \mathbb{N}})^s} \chi_1(C_1^\top \vec{k}_1 + \cdots + C_s^\top \vec{k}_s) \\
&\quad \times \chi_2(C_1^\top (\vec{k}_1 + \vec{\beta}_1(k_1)) + \cdots + C_s^\top (\vec{k}_s + \vec{\beta}_s(k_s))) \, d\mu_s(C_1, \dots, C_s) \\
&= a_0^{(1)} a_0^{(2)} + \sum_{\substack{i,j \\ (i,j) \neq (0,0)}} a_i^{(1)} a_j^{(2)} \int_{(\mathbb{Z}_q^{\mathbb{N} \times \mathbb{N}})^s} {}_q\text{wal}_i(C_1^\top \vec{k}_1 + \cdots + C_s^\top \vec{k}_s) \\
&\quad \times {}_q\text{wal}_j(C_1^\top (\vec{k}_1 + \vec{\beta}_1(k_1)) + \cdots + C_s^\top (\vec{k}_s + \vec{\beta}_s(k_s))) \, d\mu_s(C_1, \dots, C_s) \\
&= a_0^{(1)} a_0^{(2)} + \sum_{\substack{i,j \\ (i,j) \neq (0,0)}} a_i^{(1)} a_j^{(2)} \prod_{u=1}^s \int_{\mathbb{Z}_q^{\mathbb{N} \times \mathbb{N}}} {}_q\text{wal}_i(C_u^\top \vec{k}_u) {}_q\text{wal}_j(C_u^\top (\vec{k}_u + \vec{\beta}_u(k_u))) \, d\mu(C_u).
\end{aligned}$$

Since $\text{len}_q(k_u \oplus \beta_u(k_u)) > \text{len}_q(k_u)$ for at least one u it follows that \vec{k}_u and $\vec{k}_u + \vec{\beta}_u(k_u)$ cannot be strongly dependent for all u . Hence it follows from Lemma 3 that

$$\prod_{u=1}^s \int_{\mathbb{Z}_q^{\mathbb{N} \times \mathbb{N}}} {}_q\text{wal}_i(C_u^\top \vec{k}_u) {}_q\text{wal}_j(C_u^\top (\vec{k}_u + \vec{\beta}_u(k_u))) \, d\mu(C_u) = 0.$$

So

$$\mu_s(M_1(k_1, \dots, k_s) \cap M_2(k_1, \dots, k_s)) = a_0^{(1)} a_0^{(2)} = \frac{1}{q^{m+\lfloor m/2 \rfloor - 2}}$$

and

$$\mu_s(\widetilde{M}) \leq \lim_{R \rightarrow \infty} \sum_{\substack{r_1, \dots, r_s \\ r_1 + \dots + r_s \geq R}} \sum_{\substack{k_1, \dots, k_s \\ \text{len}_q(k_i) = r_i}} \frac{1}{q^{r_1 + \dots + r_s + \lfloor (r_1 + \dots + r_s)/2 \rfloor - 2}} = 0.$$

□

Lemma 5. Let $(\Omega, \mathcal{A}, \mu)$ be a measure space and let $(A_n)_{n \geq 1}$ be a sequence of sets $A_n \in \mathcal{A}$ such that

$$\sum_{n=1}^{\infty} \mu(A_n) = \infty.$$

Then the set A of points falling in infinitely many sets A_n is of measure

$$\mu(A) \geq \limsup_{Q \rightarrow \infty} \frac{\left(\sum_{n=1}^Q \mu(A_n) \right)^2}{\sum_{n,m=1}^Q \mu(A_n \cap A_m)}.$$

Proof. This is [15, Lemma 5 in Chapter I]. A proof can be found there. □

Lemma 6. Let $P \subseteq \mathbb{N}^s$ such that it does not contain any two strongly dependent elements \mathbf{k} and $\mathbf{\ell}$. Let

$$\begin{aligned} \overline{M} = \{ (C_1, \dots, C_s) \in (\mathbb{Z}_q^{\mathbb{N} \times \mathbb{N}})^s : & \nu(C_1^\top \vec{k}_1 + \cdots + C_s^\top \vec{k}_s) \leq -F(r_1, \dots, r_s) \\ & \text{for infinitely many } (k_1, \dots, k_s) \in P \}, \end{aligned}$$

where $r_i = \text{len}_q(k_i)$, and $F : \mathbb{N}_0^s \rightarrow \mathbb{N}$ is such that

$$\sum_{(k_1, \dots, k_s) \in P} \frac{1}{q^{F(r_1, \dots, r_s)}} = \infty.$$

Then

$$\mu_s(\overline{M}) = 1.$$

Proof. For given $(k_1, \dots, k_s) \in P$ let

$$M(k_1, \dots, k_s) := \{(C_1, \dots, C_s) \in (\mathbb{Z}_q^{\mathbb{N} \times \mathbb{N}})^s : \nu(C_1^\top \vec{k}_1 + \dots + C_s^\top \vec{k}_s) \leq -F(r_1, \dots, r_s)\}.$$

With the same proof as for Lemma 2 we have

$$\mu_s(M(k_1, \dots, k_s)) = \frac{1}{q^{F(r_1, \dots, r_s)-1}}$$

and hence

$$\sum_{(k_1, \dots, k_s) \in P} \mu_s(M(k_1, \dots, k_s)) = q \sum_{(k_1, \dots, k_s) \in P} \frac{1}{q^{F(r_1, \dots, r_s)}} = \infty.$$

Now we can use Lemma 5 to obtain

$$\mu_s(\overline{M}) \geq \lim_{R \rightarrow \infty} \frac{\left(\sum_{\substack{(k_1, \dots, k_s) \in P \\ r_1 + \dots + r_s \leq R}} \mu_s(M(k_1, \dots, k_s)) \right)^2}{\sum_{\substack{(k_1, \dots, k_s) \in P \\ (\ell_1, \dots, \ell_s) \in P \\ \sum \text{len}_q(k_j), \sum \text{len}_q(\ell_j) \leq R}} \mu_s(M(k_1, \dots, k_s) \cap M(\ell_1, \dots, \ell_s))}. \quad (3)$$

Proceeding in the same way as in the proof of Lemma 4 we obtain

$$\mu_s(M(k_1, \dots, k_s) \cap M(\ell_1, \dots, \ell_s)) = \mu_s(M(k_1, \dots, k_s)) \mu_s(M(\ell_1, \dots, \ell_s))$$

provided that (k_1, \dots, k_s) and (ℓ_1, \dots, ℓ_s) are not strongly dependent. But this cannot happen by the definition of the set P .

If we denote the summands of the sum in the denominator of (3) in any order by a_1, a_2, \dots, a_Q , then the expression on the right hand side of (3) can be written as

$$\lim_{Q \rightarrow \infty} \frac{\left(\sum_{k=1}^Q a_k \right)^2}{\left(\sum_{k=1}^Q a_k \right)^2 + \sum_{k=1}^Q a_k - \sum_{k=1}^Q a_k^2}. \quad (4)$$

Since $0 \leq a_k \leq 1$ for all k , and since $\lim_{Q \rightarrow \infty} \sum_{k=1}^Q a_k = \infty$ the limit in (4) is one and the result follows. \square

We need some notation. For $m \in \mathbb{N}_0$ let

$$\begin{aligned} \mathbb{Q}(q^m) &= \{x = rq^{-m} \in [0, 1) : r = 0, \dots, q^m - 1\}, \\ \mathbb{Q}^s(q^m) &= \{\mathbf{x} = (x_1, \dots, x_s) \in [0, 1)^s : x_j \in \mathbb{Q}(q^m) \text{ for } j = 1, \dots, s\}. \end{aligned}$$

Lemma 7. *Let $\mathcal{S}(C_1, \dots, C_s)$ be a digital sequence over \mathbb{Z}_q with generating matrices C_1, \dots, C_s . Let $N \in \mathbb{N}$ with q -adic expansion $N = N_{m-1}q^{m-1} + \dots + N_1q + N_0$ and let $\mathbf{x} = (x_1, \dots, x_s) \in \mathbb{Q}^s(q^m)$. Then we have*

$$D(\mathbf{x}, N) = \sum_{\substack{k_1, \dots, k_s=0 \\ (k_1, \dots, k_s) \neq (0, \dots, 0)}}^{q^m-1} \left(\prod_{j=1}^s J_{k_j}(x_j) \right) G(N, \vec{b}(k_1, \dots, k_s)),$$

where for $k = \kappa q^{a-1} + k'$ with $a \in \mathbb{N}$, $1 \leq \kappa < q$ and $0 \leq k' < q^{a-1}$ we have

$$J_k(x) = \frac{1}{q^a} \left(\frac{1}{1 - \omega_q^{-\kappa}} \overline{{}_q\text{wal}_{k'}(x)} + \left(\frac{1}{2} + \frac{1}{\omega_q^{-\kappa} - 1} \right) \overline{{}_q\text{wal}_k(x)} \right) \quad (5)$$

$$+ \sum_{c=1}^{m-a} \sum_{l=1}^{q-1} \frac{1}{q^c(\omega_q^l - 1)} \overline{{}_q\text{wal}_{lq^{a+c-1}+k}(x)} - \frac{1}{2q^{m-a}} \overline{{}_q\text{wal}_k(x)} \quad (6)$$

and for $k = 0$ we have

$$J_0(x) = \frac{1}{2} + \sum_{c=1}^m \sum_{l=1}^{q-1} \frac{1}{q^c(\omega_q^l - 1)} \overline{{}_q\text{wal}_{lq^{c-1}}(x)} - \frac{1}{2q^m},$$

and where

$$G(N, \vec{b}(k_1, \dots, k_s)) = \left[\omega_q^{b_{w+1}N_{w+1} + \dots + b_{m-1}N_{m-1}} q^w \left(\frac{\omega_q^{b_w N_w} - 1}{\omega_q^{b_w} - 1} + \omega_q^{b_w N_w} \left\{ \frac{N}{q^w} \right\} \right) \right]$$

with

$$\vec{b} = \vec{b}(k_1, \dots, k_s) = (b_0, b_1, b_2, \dots)^\top = \sum_{j=1}^s C_j^\top \vec{k}_j$$

and $w = -\nu(\vec{b})$. However, if $w \geq m$, then we put $G(N, \vec{b}) = N$.

Proof. Denote the n th element of $\mathcal{S}(C_1, \dots, C_s)$ by $\mathbf{x}_n = (x_{n,1}, \dots, x_{n,s})$. We have

$$D(\mathbf{x}, N) = \sum_{n=0}^{N-1} \left(\prod_{j=1}^s \chi_{[0, x_j)}(x_{n,j}) - x_1 \cdots x_s \right).$$

Since $x_j \in \mathbb{Q}(q^m)$ for all $j = 1, \dots, s$ it follows that the characteristic functions $\chi_{[0, x_j)}(x)$ have a finite Walsh-series representation of the form

$$\chi_{[0, x_j)}(x) = \sum_{k_j=0}^{q^m-1} J_{k_j}(x_j) \overline{{}_q\text{wal}_{k_j}(x)},$$

see [3, Lemma 3.9], with Walsh coefficients $J_{k_j}(x_j) = \int_0^{x_j} \overline{{}_q\text{wal}_k(t)} dt$. Hence we obtain

$$\begin{aligned} D(\mathbf{x}, N) &= \sum_{n=0}^{N-1} \left(\sum_{k_1, \dots, k_s=0}^{q^m-1} \left(\prod_{j=1}^s J_{k_j}(x_j) \overline{{}_q\text{wal}_{k_j}(x_{n,j})} \right) - x_1 \cdots x_s \right) \\ &= \sum_{n=0}^{N-1} \left(\sum_{\substack{k_1, \dots, k_s=0 \\ (k_1, \dots, k_s) \neq (0, \dots, 0)}}^{q^m-1} \left(\prod_{j=1}^s J_{k_j}(x_j) \right) \overline{{}_q\text{wal}_{\mathbf{k}}(\mathbf{x}_n)} \right) \\ &= \sum_{\substack{k_1, \dots, k_s=0 \\ (k_1, \dots, k_s) \neq (0, \dots, 0)}}^{q^m-1} \left(\prod_{j=1}^s J_{k_j}(x_j) \right) \sum_{n=0}^{N-1} \overline{{}_q\text{wal}_{\mathbf{k}}(\mathbf{x}_n)}. \end{aligned}$$

According to [3, Lemma 14.8] the values of J_{k_j} are of the form as given in (5) and (7), respectively. It remains to evaluate the sum $\sum_{n=0}^{N-1} {}_q\text{wal}_{\mathbf{k}}(\mathbf{x}_n)$. According to the construction of a digital sequence the q adic digits of the j th component of the n th element \mathbf{x}_n of the sequence are given by $\vec{x}_{n,j} = C_j \vec{n}$. Hence we have

$$\begin{aligned} \sum_{n=0}^{N-1} {}_q\text{wal}_{\mathbf{k}}(\mathbf{x}_n) &= \sum_{n=0}^{N-1} \prod_{j=1}^s {}_q\text{wal}_{k_j}(C_j \vec{n}_j) = \sum_{n=0}^{N-1} \prod_{j=1}^s \omega_b^{\langle \vec{k}_j, C_j \vec{n} \rangle} = \sum_{n=0}^{N-1} \omega_b^{\langle \sum_{j=1}^s C_j^\top \vec{k}_j, \vec{n} \rangle} \\ &= \sum_{n=0}^{N-1} \omega_b^{\langle \vec{b}, \vec{n} \rangle} = \sum_{n=0}^{N-1} \omega_q^{b_0 n_0 + \dots + b_{m-1} n_{m-1}}, \end{aligned}$$

where $\langle \cdot, \cdot \rangle$ denotes the usual inner product and where $\vec{b} = \sum_{j=1}^s C_j^\top \vec{k}_j$. Now we use the notation $N(w) = N_0 + \dots + N_w q^w$. Splitting up the last sum we obtain

$$\begin{aligned} \sum_{n=0}^{N-1} {}_q\text{wal}_{\mathbf{k}}(\mathbf{x}_n) &= \sum_{n=0}^{N-1} \omega_q^{b_0 n_0 + \dots + b_{m-1} n_{m-1}} \\ &= \sum_{n=0}^{q^{w+1}(N_{w+1} + \dots + N_{m-1} q^{m-w-2}) - 1} \omega_q^{n_w b_w} \omega_q^{b_{w+1} n_{w+1} + \dots + b_{m-1} n_{m-1}} \\ &\quad + \sum_{n=0}^{N(w)-1} \omega_q^{n_w b_w} \omega_q^{b_{w+1} N_{w+1} + \dots + b_{m-1} N_{m-1}} \\ &= 0 + \omega_q^{b_{w+1} N_{w+1} + \dots + b_{m-1} N_{m-1}} \sum_{n=0}^{N(w)-1} \omega_q^{n_w b_w}. \end{aligned}$$

We study the last sum. We have

$$\begin{aligned} \sum_{n=0}^{N(w)-1} \omega_q^{n_w b_w} &= \sum_{n=0}^{q^w-1} \omega_q^{0b_w} + \sum_{n=q^w}^{2q^w-1} \omega_q^{b_w} + \dots + \sum_{n=(N_w-1)q^w}^{N_w q^w-1} \omega_q^{(N_w-1)b_w} + \sum_{n=N_w q^w}^{N(w)-1} \omega_q^{N_w b_w} \\ &= q^w \sum_{k=0}^{N_w-1} (\omega_q^{b_w})^k + (N(w) - N_w q^w) \omega_q^{N_w b_w} \\ &= q^w \left(\frac{\omega_q^{b_w N_w} - 1}{\omega_q^{b_w} - 1} + \left(\frac{N(w)}{q^w} - N_w \right) \omega_q^{N_w b_w} \right) \\ &= q^w \left(\frac{\omega_q^{b_w N_w} - 1}{\omega_q^{b_w} - 1} + \omega_q^{b_w N_w} \left\{ \frac{N}{q^w} \right\} \right) \end{aligned}$$

and the result follows. \square

3 The proof of Theorem 2

Let $N \in \mathbb{N}$ with q -adic expansion $N = N_{m-1} q^{m-1} + \dots + N_1 q + N_0$. We use the representation of $D(\mathbf{x}, N)$ given in Lemma 7. For any $\mathbf{k}^* = (k_1^*, \dots, k_s^*) \in \mathbb{N}^s$ with the property that each of the k_i^* is of the form

$$k_i^* = q^{a_i^*-1} + q^{a_i^*-2} + \ell_i^*$$

with some $a_i^* \geq 3$ and some $0 \leq \ell_i^* < q^{a_i^*-2}$ we put

$$\begin{aligned} \Lambda &:= \Lambda(\mathbf{k}^*) := \sum_{\mathbf{x} \in \mathbb{Q}^s(q^m)} D(\mathbf{x}, N) {}_q\text{wal}_{\mathbf{k}^*}(\mathbf{x}) \\ &= \sum_{\substack{k_1, \dots, k_s=0 \\ (k_1, \dots, k_s) \neq (0, \dots, 0)}}^{q^m-1} \left[\prod_{j=1}^s \sum_{x_j \in \mathbb{Q}(q^m)} J_{k_j}(x_j) {}_q\text{wal}_{k_j^*}(x_j) \right] G(N, \vec{b}(k_1, \dots, k_s)). \end{aligned}$$

By the definition of the J_k and by the orthonormality of Walsh functions (see Lemma 1) we have

$$\theta(k) := \sum_{x \in \mathbb{Q}(q^m)} J_k(x) {}_q\text{wal}_{k^*}(x) = 0$$

unless we are in one of the following three cases (with $k = \kappa q^{a^*-1} + k'$ and $k^* = q^{a^*-1} + (k^*)'$):

1. k is such that $k' = k^*$, i.e., $k = \kappa q^{a^*+c-1} + k^*$ for some $c \in \mathbb{N}$ and $\kappa \in \{1, \dots, q-1\}$. In this case we have

$$\theta(k) = \frac{1}{q^{a^*+c}} \frac{1}{1 - \omega_q^{-\kappa}}.$$

2. k is such that $k = k^*$. In this case we have

$$\theta(k) = \frac{1}{q^{a^*}} \left(\frac{1}{2} + \frac{1}{\omega_q - 1} \right) - \frac{1}{2q^m}.$$

3. k is such that $k = (k^*)' = q^{a^*-2} + l^*$. In this case we have

$$\theta(k) = \frac{1}{q^{a^*}} \frac{1}{\omega_q - 1}.$$

We write $(k_j^*)' =: \tilde{k}_j = q^{a_j^*-2} + \dots$ (note that k_j^* is uniquely determined by \tilde{k}_j),

$$\begin{aligned} \beta_j(\tilde{k}_j, 0) &:= 0 \\ \beta_j(\tilde{k}_j, 1) &:= q^{a_j^*-1} \end{aligned}$$

and for $t \in \mathbb{N}_0$ and $u_j \in \{tq - t + 2, \dots, tq - t + q\}$ we put

$$\beta_j(\tilde{k}_j, u_j) = q^{a_j^*-1} + q^{a_j^*+t}(u_j - (tq - t + 1)).$$

Then for $u_j \geq 2$ we have

$$\tilde{k}_j + \beta_j(\tilde{k}_j, u_j) = (k_j^*)' + q^{a_j^*-1} + q^{a_j^*+t}(u_j - (tq - t + 1)) = k_j^* + q^{a_j^*+t}\kappa,$$

where $\kappa = u_j - (tq - t + 1)$. Hence, according to Case 1, we have

$$|\theta(\tilde{k}_j + \beta_j(\tilde{k}_j, u_j))| \leq c_1(q) \frac{1}{q^{a_j^*+t+1}} \leq c_1(q) \frac{1}{q^{a_j^*+u_j/q}}$$

for some $c_1(q) > 0$. Similarly,

$$\tilde{k}_j + \beta_j(\tilde{k}_j, 0) = (k_j^*)'$$

and hence, according to Case 3, we have

$$|\theta(\tilde{k}_j + \beta_j(\tilde{k}_j, 0))| \leq c_2(q) \frac{1}{q^{a_j^*}}$$

for some $c_2(q) > 0$, and

$$\tilde{k}_j + \beta_j(\tilde{k}_j, 1) = (k_j^*)' + q^{a_j^*-1} = k_j^*$$

and hence, according to Case 2, we have

$$|\theta(\tilde{k}_j + \beta_j(\tilde{k}_j, 1))| \leq c_3(q) \frac{1}{q^{a_j^*}}$$

for some $c_3(q) > 0$. Summing up, for all $u_j \geq 0$ we have

$$|\theta(\tilde{k}_j + \beta_j(\tilde{k}_j, u_j))| \leq c_4(q) \frac{1}{q^{a_j^* + u_j/q}} \quad (7)$$

for some $c_4(q) > 0$.

Now we have

$$\Lambda = \sum_{u_1, \dots, u_s \geq 0} \left[\prod_{j=1}^s \theta(\tilde{k}_j + \beta_j(\tilde{k}_j, u_j)) \right] G(N, \vec{b}(\tilde{k}_1 + \beta_1(\tilde{k}_1, u_1), \dots, \tilde{k}_s + \beta_s(\tilde{k}_s, u_s)))$$

where the summation is over all u_j with $\tilde{k}_j + \beta_j(\tilde{k}_j, u_j) < q^m$ for all $j = 1, \dots, s$. For any $J \in \mathbb{N}$ we have

$$\begin{aligned} |\Lambda| &\geq \left| \left[\prod_{j=1}^s \theta(\tilde{k}_j) \right] G(N, \vec{b}(\tilde{k}_1, \dots, \tilde{k}_s)) \right| \\ &\quad - \left| \sum_{\substack{0 \leq u_1, \dots, u_s \leq J \\ (u_1, \dots, u_s) \neq (0, \dots, 0)}} \left[\prod_{j=1}^s \theta(\tilde{k}_j + \beta_j(\tilde{k}_j, u_j)) \right] G(N, \vec{b}(\tilde{k}_1 + \beta_1(\tilde{k}_1, u_1), \dots, \tilde{k}_s + \beta_s(\tilde{k}_s, u_s))) \right| \\ &\quad - \left| \sum_{\substack{u_1, \dots, u_s \geq 0 \\ \exists j: u_j > J}} \left[\prod_{j=1}^s \theta(\tilde{k}_j + \beta_j(\tilde{k}_j, u_j)) \right] G(N, \vec{b}(\tilde{k}_1 + \beta_1(\tilde{k}_1, u_1), \dots, \tilde{k}_s + \beta_s(\tilde{k}_s, u_s))) \right|. \end{aligned} \quad (8)$$

Note that $|G(N, \vec{b}(k_1, \dots, k_s))| \leq qN$ always. Therefore and using (7), for the last sum in (8) we have

$$|\Sigma| \leq \frac{qN}{q^{a_1^* + \dots + a_s^*}} \sum_{\substack{u_1, \dots, u_s \geq 0 \\ \exists j: u_j > J}} q^{-\frac{u_1}{q} - \dots - \frac{u_s}{q}} \leq c_5(q, s) \frac{N}{q^{a_1^* + \dots + a_s^*}} \frac{1}{q^{J/q}},$$

with some $c_5(q, s) > 0$ depending only on q and on s .

Let the function F from Lemma 6 be such that

$$q^{F(r_1, \dots, r_s)} = q^{r_1 + \dots + r_s} (r_1 + \dots + r_s)^s \log(r_1 + \dots + r_s) \quad (9)$$

and let P from Lemma 6 be given by

$$P = \{(k_1, \dots, k_s) \in \mathbb{N}^s : (k_1, \dots, k_s) \neq (1, \dots, 1), k_i = q^{a_i-1} + \ell_i \text{ for some } a_i \in \mathbb{N} \text{ and } 0 \leq \ell_i < q^{a_i-1} \text{ for all } i = 1, \dots, s\}. \quad (10)$$

Note that in P no two elements are strongly dependent since the leading digits of the k_i are all 1. With $r = \text{len}_q(k_i)$ we have

$$\begin{aligned} \sum_{(k_1, \dots, k_s) \in P} \frac{1}{q^{F(r_1, \dots, r_s)}} &= \sum_{\substack{a_1, \dots, a_s=0 \\ a_1 + \dots + a_s \neq 0}}^{\infty} \frac{1}{q^{F(a_1, \dots, a_s)}} \sum_{\ell_1=0}^{q^{a_1}-1} \dots \sum_{\ell_s=0}^{q^{a_s}-1} 1 \\ &= \sum_{\substack{a_1, \dots, a_s=0 \\ a_1 + \dots + a_s \neq 0}}^{\infty} \frac{1}{q^{F(a_1, \dots, a_s)}} \prod_{j=1}^s \frac{q^{a_j+1} - 1}{q - 1} \\ &\geq \frac{1}{(q-1)^s} \sum_{\substack{a_1, \dots, a_s=0 \\ a_1 + \dots + a_s \neq 0}}^{\infty} \frac{1}{(a_1 + \dots + a_s)^s \log(a_1 + \dots + a_s)} \\ &= \frac{1}{(q-1)^s} \sum_{d=1}^{\infty} \frac{1}{d^s \log d} \binom{s+d-1}{d} \\ &\geq \frac{1}{(q-1)^s} \frac{1}{(s-1)!} \sum_{d=1}^{\infty} \frac{1}{d \log d} \\ &= \infty, \end{aligned}$$

where we used that $\binom{s+d-1}{d} \geq \frac{d^{s-1}}{(s-1)!}$.

Now we use Lemma 6 and find that the set \overline{M} for our choice of F as in (9) and P as in (10) has measure $\mu_s(\overline{M}) = 1$.

Next we consider the finite collection of s -tuples

$$(\beta_1(k_1, u_1), \dots, \beta_s(k_s, u_s))$$

for $u_1, \dots, u_s = 0, 1, \dots, J$ but not all equal to 0. Note that each of these $\beta_i(k_i, u_i)$ is either 0 or has $\text{len}_q(\beta_i(k_i, u_i)) > \text{len}_q(k_i)$ for each (k_1, \dots, k_s) which is an element from P defined above.

Now we use Lemma 4 where we choose \overline{P} as $\overline{P} = P$ from (10) and for any choice of $u_1, \dots, u_s = 0, 1, \dots, J$ but not all equal to 0, we choose the $\beta_i(k_i)$ from Lemma 4 as $\beta_i(k_i) = \beta_i(k_i, u_i)$. Then for the corresponding set $\widetilde{M} := \widetilde{M}(u_1, \dots, u_s)$ of Lemma 4 we have $\mu_s(\widetilde{M}) = 0$.

We set

$$M := \overline{M} \setminus \bigcup_{\substack{u_1, \dots, u_s=0 \\ (u_1, \dots, u_s) \neq (0, \dots, 0)}}^J \widetilde{M}(u_1, \dots, u_s)$$

and find that $\mu_s(M) = 1$.

Now we make a suitable choice for C_1, \dots, C_s and for \mathbf{k}^* . Let $(C_1, \dots, C_s) \in M$ and let $(\widetilde{k}_1, \dots, \widetilde{k}_s) \in P$ be such that

$$\nu(C_1^\top \vec{\widetilde{k}}_1 + \dots + C_s^\top \vec{\widetilde{k}}_s) \leq -F(r_1, \dots, r_s) \leq -(r_1 + \dots + r_s)$$

and

$$\nu(C_1^\top(\vec{k}_1 + \vec{\beta}_1(\tilde{k}_1, u_1)) + \cdots + C_s^\top(\vec{k}_s + \vec{\beta}_s(\tilde{k}_s, u_s))) \geq -\frac{r_1 + \cdots + r_s}{2},$$

where $r_i = \text{len}_q(\tilde{k}_i)$ and $\tilde{k}_i = q^{\tilde{a}_i-1} + \tilde{\ell}_i$. By the definition of M there are infinitely many such s -tuples $(\tilde{k}_1, \dots, \tilde{k}_s)$.

Let $m := \lfloor F(r_1, \dots, r_s) \rfloor$ and $N = q^{m-1}$. We analyze the first summand in (8): Let

$$C_1^\top \vec{k}_1 + \cdots + C_s^\top \vec{k}_s = (0, \dots, 0, b_w, b_{w+1}, \dots)^\top$$

with $b_w \neq 0$. Then we have

$$-w = \nu((0, \dots, 0, b_w, b_{w+1}, \dots)^\top) = \nu(C_1^\top \vec{k}_1 + \cdots + C_s^\top \vec{k}_s) \leq -F(r_1, \dots, r_s) \leq -m$$

and hence $w \geq m$. This means that $G(N, \vec{b}(\tilde{k}_1, \dots, \tilde{k}_s)) = N$ and hence we obtain

$$\left| \left[\prod_{j=1}^s \theta(\tilde{k}_j) \right] G(N, \vec{b}(\tilde{k}_1, \dots, \tilde{k}_s)) \right| \geq c_6(q, s) \frac{N}{q^{\tilde{a}_1 + \cdots + \tilde{a}_s}}.$$

Now we turn to the second summand in (8). Let

$$C_1^\top(\vec{k}_1 + \vec{\beta}_1(\tilde{k}_1, u_1)) + \cdots + C_s^\top(\vec{k}_s + \vec{\beta}_s(\tilde{k}_s, u_s)) = (0, \dots, 0, b_w, b_{w+1}, \dots)^\top$$

with $b_w \neq 0$. Then we have

$$\begin{aligned} -w &= \nu((0, \dots, 0, b_w, b_{w+1}, \dots)^\top) \\ &= \nu(C_1^\top(\vec{k}_1 + \vec{\beta}_1(\tilde{k}_1, u_1)) + \cdots + C_s^\top(\vec{k}_s + \vec{\beta}_s(\tilde{k}_s, u_s))) \\ &\geq -\frac{r_1 + \cdots + r_s}{2} \end{aligned}$$

and hence

$$w \leq \frac{r_1 + \cdots + r_s}{2}.$$

This means that

$$\begin{aligned} |G(N, \vec{b}(\tilde{k}_1 + \beta_1(\tilde{k}_1, u_1), \dots, \tilde{k}_s + \beta_s(\tilde{k}_s, u_s)))| &\leq c_7(q) q^w \\ &\leq c_7(q) q^{\frac{r_1 + \cdots + r_s}{2}} \\ &= c_8(q, s) q^{\frac{\tilde{a}_1 + \cdots + \tilde{a}_s}{2}} \end{aligned}$$

and hence we obtain

$$\begin{aligned} \left| \sum_{\substack{u_1, \dots, u_s \geq 0 \\ \exists j: u_j > J}} \left[\prod_{j=1}^s \theta(\tilde{k}_j + \beta_j(\tilde{k}_j, u_j)) \right] G(N, \vec{b}(\tilde{k}_1 + \beta_1(\tilde{k}_1, u_1), \dots, \tilde{k}_s + \beta_s(\tilde{k}_s, u_s))) \right| \\ \leq c_9(q, s) \frac{q^{\frac{\tilde{a}_1 + \cdots + \tilde{a}_s}{2}}}{q^{\tilde{a}_1 + \cdots + \tilde{a}_s}}. \end{aligned}$$

Altogether we have

$$\begin{aligned} |\Lambda| &\geq c_6(q, s) \frac{N}{q^{\tilde{a}_1 + \dots + \tilde{a}_s}} - c_9(q, s) \frac{q^{\frac{\tilde{a}_1 + \dots + \tilde{a}_s}{2}}}{q^{\tilde{a}_1 + \dots + \tilde{a}_s}} - c_5(q, s) \frac{N}{q^{a_1^* + \dots + a_s^*}} \frac{1}{q^{J/q}} \\ &\geq c_{10}(q, s) \frac{N}{q^{\tilde{a}_1 + \dots + \tilde{a}_s}} \end{aligned}$$

for J large enough and for $\text{len}_q(\tilde{k}_1) + \dots + \text{len}_q(\tilde{k}_s)$ large enough. Now

$$\begin{aligned} \frac{N}{q^{\tilde{a}_1 + \dots + \tilde{a}_s}} &\geq c_{11}(q, s) q^{F(r_1, \dots, r_s) - r_1 - \dots - r_s} \\ &= c_{11}(q, s) (r_1 + \dots + r_s) \log(r_1 + \dots + r_s) \\ &\geq c_{12}(q, s) (\log N)^s \log \log N. \end{aligned}$$

From the definition of Λ it follows that there exists an $\mathbf{x} \in \mathbb{Q}^s(q^m) \subseteq [0, 1]^s$ such that

$$|D(\mathbf{x}, N)| \geq c_{13}(q, s) (\log N)^s \log \log N$$

and the proof of Theorem 2 is finished. \square

References

- [1] J. Beck: Probabilistic diophantine approximation, I. Kronecker-sequences. *Ann. Math.* 140: 451–502, 1994.
- [2] J. Beck and W. W. L. Chen: *Irregularities of Distribution*. Cambridge University Press, Cambridge, 1987.
- [3] J. Dick and F. Pillichshammer: *Digital Nets and Sequences. Discrepancy Theory and Quasi-Monte Carlo Integration*. Cambridge University Press, Cambridge, 2010.
- [4] M. Drmota and R.F. Tichy: *Sequences, Discrepancies and Applications*. Lecture Notes in Mathematics 1651, Springer-Verlag, Berlin, 1997.
- [5] H. Faure: Discrépance de suites associées à un système de numération (en dimension s). *Acta Arith.* 41: 337–351, 1982.
- [6] H. Faure: Discrepancy lower bound in two dimensions. In: *Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing*. Lecture Notes in Statist. 106, Springer, 1995, 198–204.
- [7] L. Kuipers and H. Niederreiter: *Uniform Distribution of Sequences*. John Wiley, New York, 1974; reprint, Dover Publications, Mineola, NY, 2006.
- [8] G. Larcher: On the distribution of digital sequences. In: *Monte Carlo and Quasi-Monte Carlo Methods 1996 (Salzburg)*, vol. 127 of Lecture Notes in Statistics, pp. 109–123, Springer, New York, 1998.
- [9] J. Matoušek: *Geometric discrepancy. An illustrated guide*. Algorithms and Combinatorics, 18. Springer-Verlag, Berlin, 1999.

- [10] H. Niederreiter: Point sets and sequences with small discrepancy. *Monatsh. Math.* 104: 273–337, 1987.
- [11] H. Niederreiter: *Random Number Generation and Quasi-Monte Carlo Methods*. SIAM, Philadelphia, 1992.
- [12] K.F. Roth: On irregularities of distribution. *Mathematica* 1: 73–79, 1954.
- [13] W.M. Schmidt: Irregularities of distribution VII. *Acta Arith.* 21: 45–50, 1972.
- [14] I.M. Sobol: The distribution of points in a cube and the approximate evaluation of integrals. *Zh. Vychisl. Mat. i Mat. Fiz.* 7: 784–802, 1967.
- [15] V. G. Sprindžuk: *Metric Theory of Diophantine Approximations*. Scripta Series in Mathematics. V. H. Winston & Sons, Washington, D.C.; A Halsted Press Book, John Wiley & Sons, New York-Toronto, Ont.-London, 1979.

Authors' address:

Gerhard Larcher, Friedrich Pillichshammer

Institut für Finanzmathematik, Universität Linz, Altenbergerstr. 69, 4040 Linz, Austria

E-mail:

`gerhard.larcher@jku.at`,

`friedrich.pillichshammer@jku.at`